

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-40. (cancelled)

41. (new) A method for trusting sites in a communication network, comprising:

receiving at least one input credential to authenticate a site;

feeding said at least one input credential to an advanced policy to deduce a plurality of verified general-context declarations related to said site in addition to the authentication of said site, wherein if said plurality of verified general-context declarations cannot be deduced,

receiving at least one additional input credential, and feeding said at least one additional input credential to said advanced policy to deduce a plurality of verified general-context declarations related to said site in addition to the authentication of said site, until a plurality of verified general-context declarations related to said site in addition to the authentication of said site are deduced;

associating a symbol with each one of said plurality of verified general-context declarations; and

displaying said symbol in a predefined way that cannot be set by said site,

wherein said advanced policy is deducing said plurality of verified general-context declarations as a function of at least one existing credential known to said advanced policy, or to said at least one input credential or said at least one additional input credential.

42. (new) The method according to claim 41, wherein said at least one additional input credential is related to said site.

43. (new) The method according to claim 41, wherein said at least one additional input credential is related to an entity known to said advanced policy.

44. (new) The method according to claim 41, wherein said step of receiving said at least one input credential to authenticate said site further comprises applying an SSL authenticating protocol.

45. (new) The method according to claim 41, wherein at least one said symbol is displayed in a trusted pane.

46. (new) The method according to claim 45, wherein said displaying further comprises displaying in a two pane mode at least one original site page in a first pane from among said two panes and said at least one symbol in a trusted pane from among said trusted pane.

47. (new) The method according to claim 41, wherein said general-context declaration that corresponds to one of said symbols being that the site is sex free.

48. (new) The method according to claim 41, wherein said general-context declaration that corresponds to one of said symbols being that the site is violence free.

49. (new) The method according to claim 41, wherein said credential being a certificate or certificate chain.

50. (new) A method according to claim 41, wherein said advanced policy includes a role assignment module.

51. (new) A system for trusting sites in a communication network, the communication network including a plurality of user nodes inter-linked through at least one proxy node to at least one site server, the system comprising:
at least one user accessing from a user node,
through a proxy node to a server site;

the server site providing to said proxy node, through said communication network, at least one input credential;

the proxy node feeding said at least one input credential to an advanced policy to deduce a plurality of verified general-context declarations related to said site in addition to the authentication said site, wherein if said plurality of declarations cannot be deduced, the proxy node receiving at least one additional input credential and feeding said at least one additional input credential to said advanced policy until a plurality of verified general-context declarations related to said site in addition to the authentication of said site are deduced;

the proxy node associating a symbol with each one of said plurality of verified general-context declarations; and

the proxy node sending the symbol to the user node and the user displaying said symbol in a predefined way that cannot be set by said site,

wherein said advanced policy is deducing said plurality of verified general-context declarations as a function of at least one existing credential known to said advanced policy, or to said input credential or said at least one additional input credential.

52. (new) The system according to claim 51, wherein said user node includes a browser.

53. (new) The system according to claim 51, wherein said user node being cellular telephone.

54. (new) The system according to claim 51, wherein said user node being Personal Digital Assistance device.

55. (new) The system according to claim 51, wherein said proxy node is executed on each of said at least one user node, respectively.

56. (new) The system according to claim 51, wherein the proxy node is configured in response to said advanced policy, to collect additional credentials from credential repository.

57. (new) The system according to claim 51, wherein said at least one input credential is related to said site.

58. (new) The method according to claim 51, wherein said at least one additional input credential is related to an entity known to said advanced policy.

59. (new) A computer software product, including a computer-readable medium in which computer program instructions are stored, which instructions, when read by a

computer, cause the computer to perform a method for trusting sites in a communication network, comprising:

receiving at least one input credential to authenticate a site;

feeding said at least one input credential to an advanced policy to deduce a plurality of verified general-context declarations related to said site in addition to the authentication of said site, wherein if said plurality of verified general-context declarations cannot be deduced,

receiving at least one additional input credential, and feeding said at least one additional input credential to said advanced policy to deduce a plurality of verified general-context declarations related to said site in addition to the authentication of said site, until a plurality of verified general-context declarations related to said site in addition to the authentication of said site are deduced;

associating a symbol with each one of said plurality of verified declarations; and

displaying said symbol in a predefined way that cannot be set by said site,

wherein said advanced policy is deducing said plurality of verified general-context declarations as a function of at least one existing credential known to said

advanced policy, or to said input credential or said at least one additional input credential.

60. (new) The method according to claim 59, wherein at least one of said symbol is displayed in a trusted pane.